Search

Recent Posts

What Is Email Security and Are You Doing It Right?

What Are Malware Bots and How to Get Rid of Them?

Top Five Security Apps for Android Mobile Devices in 2019

Top 5

How to Recognize Suspicious Applications and Improve Mobile Cybersecurity?

August 5th, 2019 sumana Hardware, Security, Social Media, Technology and IT Tips, Web & Cloud App Store, Business, cybersecurity, data, Google, hackers, Hardware, internet, Malware, NIST Framework, Orange County IT Support, ransomware, The Network Pro, tips

Mandatory Security Measures for Windows Users

Cybersecurity and Startups – The First Steps to Securing Your Business

Categories

Select Category

Archives

Select Month

The mobile application market currently has billions of smartphone apps in dozens of different categories including games, productivity apps, scheduling apps, and social media networks. With so many apps available on the Google Play Store and Apple's App Store, users can easily access any type of service they need. However, most of them forget that even applications can be major security risks that can cause serious consequences such as identity theft. Here are five tips on how you can recognize suspicious application!

#1 Recognize Inappropriate Permissions

Whenever you download an app, it will ask you to give certain permissions so the app can function correctly. For example, a video messaging app would require your permission to use your camera, which is completely normal. However, if you pay attention to the permissions you are being asked for, you can easily tell whether an application is legit or not. For example, if you're downloading a game that doesn't require your content whatsoever but the app

asks for permission to access your photo gallery, it might be a sign that you've come across a suspicious application. If the permissions don't match the app, uninstall it right away.

#2 Check E-Mail Contacts of the App Developers

If you want to be extra careful when downloading apps, make sure to check the contact email of the app developer. Professional developers always have professional emails that usually look something like this: professional@developer.com. However, amateurs and potential hackers don't have professional email addresses and they often use free email services such as Gmail, Yahoo, or Hotmail. If the developer's contact email ends with one of these three, it's a reason to believe that the app might not be legit.

#3 Don't Download Apps Outside the App

Store

If you want to improve your online security and keep your data safe, never download smartphone apps from illegitimate sources other than the official app stores. Google Play Store and Apple's App Store scan each app for malware and check whether each app is safe to use. Other sources rarely implement these kinds of security checks, which means you are more likely going to come across a malicious app. Therefore, if the app is not available in one of the official app stores, then it's best to stay away from it.

#4 Check for Poor App Descriptions

Fake apps or apps designed for malicious purposes often have bad descriptions and content. Many hackers come from third world countries and don't have a good understanding of the English language. Others just don't want to put too much effort into the fake app. That's why these apps often have poor descriptions with many spelling and grammar errors. Some even have bad photos and suspicious reviews that look like they've been purchased or faked. Make sure to keep an eye out for these

suspicious traits and watch out for spelling errors because they're often a sign that something doesn't align. A professionally designed app would never have a poor description.

#5 Recognize Bad Visuals

Lastly, learn to recognize a fake or malicious app by observing its visuals. Most fake apps have very poor visual because hackers don't put too much effort into the design. All they want is for you to download the app so they can get access to your data. Bad visuals include strange fonts, oversize letters, and poor-quality images.

Conclusion

Hackers use malicious apps to gain access to people's confidential data. By downloading such an app, you are opening the door to anyone who wants to steal your data for malicious purposes. However, if you stay aware of the potential risks, you will be able to keep your devices protected. Make sure to look into the NIST cybersecurity framework for extra security measures!

← Older

Next →

Spend 20 minutes with our president Kevin Studley. You will leave that meeting with a completely different perspective on your business costs and risks associated with technology.

STAY IN TOUCH

180 N. Riverview Drive, Suite 300 Anaheim, CA 92808

☎ 714-333-9620

SUBSCRIBE

NAVIGATION

5 Reasons Why
Services & Solutions
Blog
Resources
About Us

SOCIAL MEDIA

Twitter
Facebook
Google
LinkedIn
RSS

First name

Last name

Email*

Dream100

protected by reCAPTC

Privacy - Terms

Submit